IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 9, Issue 8, August 2021

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.542

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.542

|| Volume 9, Issue 8, August 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0908021 |

Attribute Based Access Control for ICN Naming Scheme

Mr. Sachin M. Gaikwad[1], Prof. Ankush Pawar[2], Prof. Ankit S. Sanghvi[3]

PG Student, Department of Computer Engineering, ARMIET, Maharashtra, India[1]

Associate Professor, Department of Computer Engineering, VPS, Maharashtra, India[2]

Assistant Professor, Department of Computer Engineering, ARMIET, Maharashtra, India[3]

ABSTRACT - The new ICN network design aims to solve the vulnerability of the old IP basis networking architecture. Instead of constructing a connection between communication hosts, the ICN focusses on content, i.e. data, transmitted to the network. In different locations, copies of the content can be cached in ICN. Once it has been published, the content is beyond the control of its owner. Therefore, it is essential in ICN to enforce access control regulations for distributed content copies. Attribute-Based Encryption (ABE) is a viable solution in this setting to implement such control mechanics. However, two obstacles arise in the application of ABE in ICN: Complications of management in distributed attribute management; all ICN users are published in terms of privacy protection under the enforced policy on content access in contrast to traditional networks. Therefore, it should not be allowed to retrieve the access policies from unlawful content readers. To this purpose, this article presents ICN's privacy-conserving access control method and its corresponding attribute management solution. The technique described is consistent with the current ICN architectures based on flat names.

KEYWORDS: privacy, naming, information centric networking, access control, attribute management.

I. INTRODUCTION

In traditional networking schemes, if a network entity wants to access some information content, it has to locate and connect to the server that provides such service following network routing protocols. As a result, the information is tightly associated with the location of the server. The entire network is centered on the connections between content consumers and content providers, making connection status an important factor to the network.Witnessed by the fact that most of the network traffic is file sharing, especially video sharing, various ICN architectures are proposed. In ICN architecture, the focus is shifted from consumer-server connections to consumer-content connections. Thus, instead of identifying the content owner's address, the network changes to identify authentic content copies. In this way, the consumers do not need to know where the content locates, i.e. the IP address of the content owner. The content name is sufficient to direct the consumer to a content copy. Content owners publish the content, which can be copied and stored in the network using network caches. This design enables contents being efficiently delivered to consumers.Though the design is efficient in retrieving content, it brings great challenges to security issues during content caching and retrieving. One of them is that traditional access control mechanisms cannot be easily enforced. This is because, in ICN, content owners and consumers are not directly connected. Content owners have no control over the distributed network caches. To enforce access control to the content, several frameworks have been proposed. Most of them require additional authorities or secure communication channels in network to authenticate each content consumer. These schemes are sound but have too much reliance on traditional control schemes, making them inefficient in practice.

The Internet is built on the connecting service of the IP protocol intrinsically to perform end-to-end interactions between hosts. The user must therefore indicate the server for data extraction. Today, the transfer of information over the Internet and the need for information from customers might increase significantly. This is a great fit to customer-side technologies such as HTTP, FTP, telnet and SMTP. However, host-centered Internet infrastructure, which requires a paradigm shift inside historical content delivery frameworks, is ideal for inefficient bandwidth-intensive modern Internet usage patterns. Two-stage modeling needs overhead utilization The IP address is already linked to the location, which does not permit nodes and application mobility Safety is yet another major challenge, because the host is tightly associated with the security system. Hosts thus become the focal point of various concerns to security. Furthermore, while the IP router is

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.542

|| Volume 9, Issue 8, August 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0908021 |

stateless and does not supply storage power, the same demand has been generated several times throughout the route and would lead to overuse of bandwidth. It led to analyzes on the move from the host to the information-centered Internet structure. Past techniques like Content Delivery Networks and Peer-to-Peer explore similar difficulties to enhance user access. These shortcomings have encouraged the research community to look for new internet alternative technologies. ICN's principal goal was to turn the present host-oriented manner of communication into a content-centered framework. After it has been printed, the material is beyond the owner's control. It is therefore vital for ICN to enforce the shared content copy authentication policies.

II. LITERATURE REVIEW

Zhongma Zhu & Rui Jiang (2016) has established for dynamic members a safe data sharing system. By not using the communication channels, a safe approach for key distribution was implemented. This system was kept out of collusion attacks, in which revoked users failed in combining with an untrusted cloud to reach their original data file. When a new user was attached or departed in a group, the proposed system did not update the private keys. However, for safe data transfer, the memory usage was significant.

Chavhan Bhaurao and Deshmukh Swati (2015) introduces a safe, multi-owner cloud data sharing system. Using the Group signature and dynamic encryption methods, the cloud user shared the data. The overhead storage and calculation were not necessary. However, the overhead of the storage employing safe, multi-owner data-sharing techniques was not lowered to some level.

Mazhar Ali et al. (2015) strengthened confidentiality of data, integrity, access control, data sharing and threat security in cloud-based data sharing (SeDaSC) technique. Single encryption key is used for the SeDaSC approach. With user share, two distinct key shares were formed for each user. The unique share of SeDaSC's key methodology for countering insider threats was assigned. A trusted third party called the cryptography server saved an additional key share. However, the data sharing in clouds did not address the throughput.

Bojan Suzic and other collaborative infrastructures were secured through the private cloud federation (2015). The characteristics of access control, data and security policy languages have been investigated. The characteristics allow fine grain security and semi-conscious data processing. As interoperability across heterogeneous infrastructures and services, the principal issues were provided. The main goal was to ensure the requirements of the public sector compliance with security and legal transparency and privacy.

Shulan Wang et al. (2016) devised an attribute-based data sharing system to deal with CC apps' key escrow problem. The key authority and CSP cooperated with the private user key using an upgraded two-party key issuance mechanism. The ideas with weight attributes enhance the attribute expression and increase the expression from binary to arbitrary. The secrecy of data was however not improved utilizing a data sharing strategy based on attributes.

Qinlong Huang et al. (2015) in CC was a model of an Efficient Efficient Revocation Secure Data Sharing Method (EABDS). In order to allow the data secrecy and achieve a fine graining access control, a symmetrically encrypted data with the Data Encryption Key (DEK) was encrypted with the designed technique. The technique employed homomorphic encryption to make the user's secret key attribute using the key server attribute authority. The designed system eliminated the attribute authority through secret key generation from data access. A mechanism for revoking the attribute immediately achieved reverse and forward security. However, the key generation time was not lowered with a secure data exchange system based on attributes.

Marimuthu et al. (2014) intended to create a dynamic cloud group with Secure Multi-Owner Data Sharing system. The cloud user offers data for other users using group signature and broadcast encryption techniques. The overhead storage and computing costs for the system have not been predicated on the number of users removed. One-time password used to secure access was an authentication technique. A one-time password for installing across machines was a secure type of authentication. The data sharing, however, was not performed safely.

III. OBJECTIVE

Relevant objective of the proposed system are a s follows

1. The main objective is to provide the data and privacy protection.
2. To ensure the protection of cloud database.
3. To perform secure and efficient processing.
4. To provide a better control on data encryption and sharing

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.542

|| Volume 9, Issue 8, August 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0908021 |

In contrast to previous studies, our work focuses on access management solutions in NDN. Compatible with (where writers investigate the safety, privacy and access control from a bird's-eye perspective) we explore and review ICN/existing NDN1's access control mechanisms. We further categorize existing solutions into two main groups, followed by a set of subcategories for each category.

The main contributions of our study in this connection are:

1. We examine security, encryption techniques and security protocols on the basis of content, and access control for NDN.
2. We conduct a detailed examination of NDN access control methods (including encryption based and independent encryption solutions).
3. We outline future issues for access control in NDN and research directions.

IV. PROBLEM DEFINITION

We propose an ICN naming system attribute-based access control. The scheme proposed can be separated into two levels. At the highest levels, the dispersed attributes within the ICN network are managed via an ontology-based solution for the management of attribute challenges. This technique can more effectively combine the qualities declared by different authorities than traditional ways. Consumers do not have to negotiate their attribute keys when seeking content from other authorities.

It offers ontological attribute management, reducing the cost of managing attributes in distributed deployment significantly. The proposed management technique allows adjustable combinations of access control policy operations; allows for ranking and privilege access management and allows flexible building of a real-world access policy. The policy regarding access to content is maintained privately. The ICN NETATE system, which combines flexibles management of attributes and privacy policies to safeguard access, considerably decreases the overhead to allow potential customers to verify their eligibility for access to material.

V. PROPOSED SYSTEM

Different ICN architectures are proposed, as shown by the sharing of files, especially in relation to the sharing of video. The focus is changed from consumer servers to consumer content in ICN architecture. The network is therefore capable of recognizing valid copies of content instead of the address of the owner. This means that consumers do not need to know where the content is located, i.e. the IP address of the content owner. The name of the content is sufficient to link the consumer to a copy of the material. The content owners publish the content, which can be copied and stored via network caches. This architecture allows the delivery of contents to users efficiently.

Although the approach is efficient in the recovery of content, security considerations during the caching and retrieval of content are big challenges. One is that it is not easy to implement typical access control measures. Because the ICN does not directly connect content owners and consumers. Content proprietors have no influence over network caches delivered. Several approaches have been proposed for enforcing content access control. In most circumstances, any content consumer must be authenticated by additional authorities or secure network communications channels. These are good systems, but they are too dependent on conventional controls and virtually inefficient.

In our approach, each network entity is assigned with a set of attributes with the help of a Trusted Third Party (TTP) according to their real identities. The access control policy is enforced according to the content names instead of the contents. Moreover, privacy-preservation is provided for the content access policies. This feature can greatly improve the privacy protection on ICN data when they are distributed in the public domain. In this way, a user is able to identify its eligibility of the accessed contents through the encrypted names before actually accessing the data content. To further support the use of ontology in attribute management, the proposed scheme enables comparison between attributes, which gives the capability to rank attributes and associate different privileges accordingly. In summary, the work can be listed as follows:

1. It provides ontology-based attribute management, which greatly reduces the cost for attribute management in distributed deployment. The proposed management scheme supports flexible attribute combination operations in access control policies.
2. It enables attribute rankings and access privilege management, making it flexible to construct a data access policy in real-world scenario. The content access policy is confidentially preserved. Ineligible consumers cannot derive the data access policies even if they collude together.
3. It proposes a naming scheme for ICN network which combines the flexible attribute management solution with the privacy preserving access policy.
4. It significantly reduces the computation and communication overhead for a potential consumer to determine his eligibility to access the content.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.542

|| Volume 9, Issue 8, August 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0908021 |

Cipher text-based attribute encryption (CP-ABE) in our proposed system is an innovative method that enables data owners directly to control outsourced data with finely structured, cryptographic access. They add security for accessing our cloud in the data owner and consumer login. OTP will be the four-digit number for one-time password. It is produced via the email. It checks whether or not the same OTP occurs. This OTP is regarded as a login password. The only way to access our cloud ICN server is to match OTP. Use the ICN security cloud server. The study proposes a safe and cost-effective data access control for cloud storage ICN systems based on attributes. In principle, we construct a CP-ABE Framework for several authorities, which includes: No fully authorized central authority may be required in a scheme, and every authority may individually offer the users secret keys.

1. Each authority for attributes may exclude any user automatically from its jurisdiction so that those removed users will no longer have access to the outsourced information.
2. In such a way that revoked Users cannot use previously available information, ICN Server may update encrypted data from current time-line to new data.
3. Secret keys updates and encrypted content are publicly available

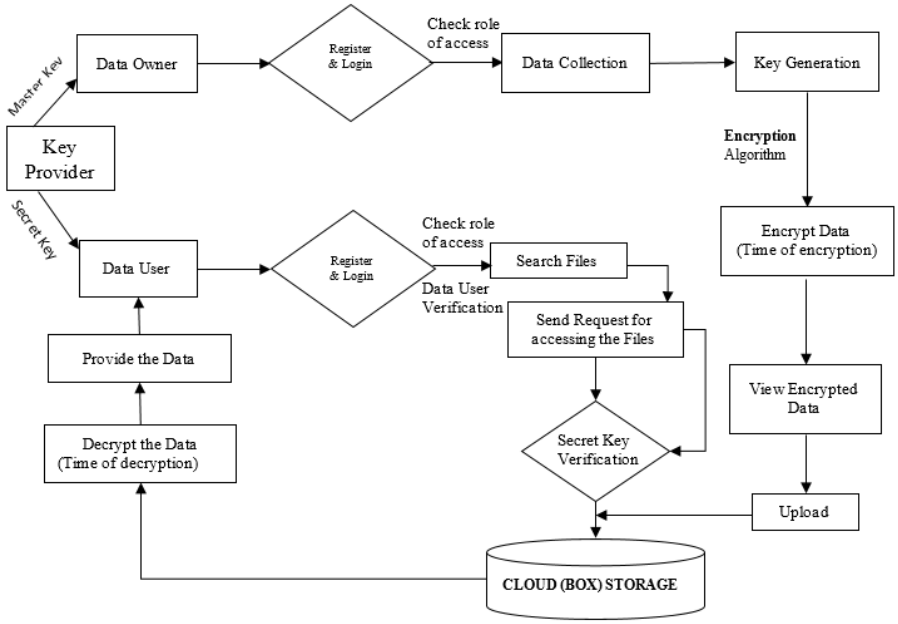


Figure No-1: Data Flow Diagram

VI. DESIGN DETAIL

a) Data Owner and Data User Login

The overall patient records is maintained by the data owner. The data owner can login with their username and password if it is valid, it will be redirected to the another form. The data owner will manage all the patient details. The user can login with their username and password if it is a new user, the user have to be registered before login. Then the data user will search a record to download. After getting an approval from server, the data user will download the records.

b) Key Provider : Giving key to user and owner:

While registration the owner and user would get the secret key from the access provider

c) Data Selection and Loading

Data selection is the process of selecting the appropriate data set for processing. The dataset, which contains all the information about the patient healthcare records. The healthcare records are selected for securely maintaining all the patient details.

d) Key Generation

Key generation is the process of generating keys in cryptography. A key is used to encrypt and decrypt whatever data is being encrypted/decrypted. The algorithm is used for generating a key for encrypting the patient healthcare records.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.542

|| Volume 9, Issue 8, August 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0908021 |

e) Data Encryption and Upload

Encryption is the most effective way to achieve data security. To read an encrypted file, the data user must have access to a secret key that enables us to decrypt it. Unencrypted data is called plain text; encrypted data is referred to as cipher text. The Encryption algorithm is used for encrypting the data. Finally, the encrypted data's are uploaded into the cloud server for secure maintenance.

f) Cloud Service Provider

The Cloud Service Provider can view all the uploaded and downloaded documents in the Cloud. The CSP receives the document request from the Data User, verifies the authentication before granting permission. Then the CSP executes the query and returns the encrypted document according to the search token. In addition, returns an additional proof with the document, to verify the search result.

g) Public Verification Key

Public verification key is a security measure designed to make sure that your document outsourced in cloud is not hacked. By verifying public key, the Data Owner and the Data User adding another layer of protection to the documents or files in the cloud by confirming each other's identities.

h) Data User

Data User send a request to the cloud server. After request granted from the Cloud, the Data User receiving the Public Verification Key from the Cloud generated by Data Owner. The Data User now decrypt and download the encrypted documents, after verifying with the Public Verification Key. After receiving a verification from cloud, the data user will download the file within a particular time limit.

i) Verification with Proof Index

It is a proof generating system for verifying cloud search by Public Verification Key; here the data users or others can verify the correctness of the search result by Verification key.

j) Decryption

The conversion of encrypted data into its original form is called Decryption. It is generally a reverse process of encryption. It decodes the encrypted information so that an authorized user can only decrypt the data because decryption requires a secret key.

k) Download Patient Records

After the successful verification of secret key, the data user will download the patient healthcare records. Finally, all the records are securely decrypted and send to the user.

VII. ALGORITHMS USED

In the proposed scheme, a **GlobalSetup** algorithm is run by the TTP to generate global parameters for the system. For each node joining in the network, the TTP runs **NodeJoin** algorithm once to generate a unique secret for the node. For each attribute, the authority in charge runs an **AuthoritySetup** algorithm to generate secrets associated with that attribute. Besides, this naming scheme includes other three basic algorithms: **KeyGen**, **Encrypt**, and **Decrypt**. Once set up, the authority of an attribute runs **KeyGen** for each node carrying this attribute to allocate the inherent attribute secrets. **Encrypt**

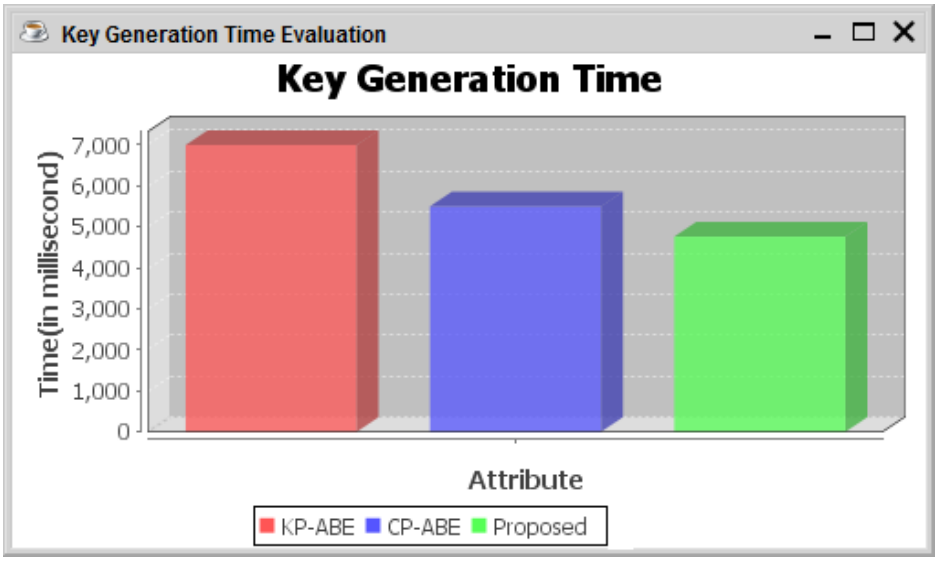
VIII. RESULTS AND DISCUSSION

Finally we have received the varies results, In this, we are comparing the performance of proposed system with the existing system with the help of Bar Graph while comparing different attributes those are: Key Generation time and the results are as below.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.542

|| Volume 9, Issue 8, August 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0908021 |



Final results analysis graph of computation performance of decryption, encryption, and key generation is shown in following figure no 2

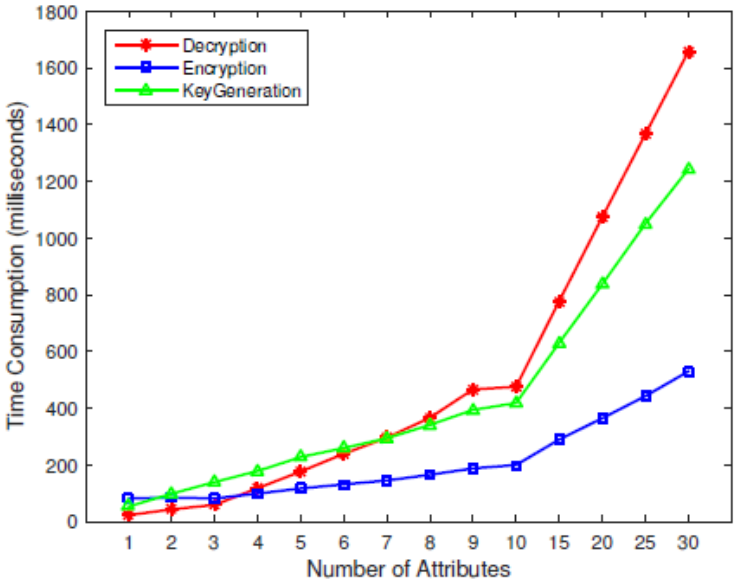


Figure No-2: Computation Performance

IX. CONCLUSION

In this system, we proposed a comprehensive access control solution for ICN network. This solution is based on an ontology-based attribute management scheme and a privacy-preserving ABE-based naming scheme. The ontology-based scheme supports flexible attribute management with significant performance gains in terms of time consumption, storage costs, and throughput improvement. From security and privacy perspective, the ABE-based naming scheme achieves a high security level as CP-ABE, but with attribute anonymity protection for policy privacy and flexible attribute rankings. The attacker cannot break the encryption algorithm to get any data exposed. Furthermore, it is also proved that attackers cannot conduct collusion attacks onto the system.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.542

|| Volume 9, Issue 8, August 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0908021 |

REFERENCES

[1] Cisco, "Cisco visual networking index: forecast and methodology, 2012-2017," 2013.
[2] A. Carzaniga, M. Rutherford, and A. Wolf, "A routing scheme for content-based networking," in INFOCOM 2004.
[3] T. Koponen, M. Chawla, B.-G. Chun, A. Ermolinskiy, K. H. Kim, S. Shenker, and I. Stoica, "A dataoriented (and beyond) network architecture," in SIGCOMM, 2007.
[4] C. Dannewitz, J. Golic, B. Ohlman, and B. Ahlgren, "Secure naming for a network of information," in INFOCOM 2010.
[5] N. Fotiou, P. Nikander, D. Trossen, and G. Polyzos, "Developing information networking further: From psirp to pursuit," ser. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, 2012.
[6] "Named data networking," 2015. [Online]. Available: http://named-data.net
[7] I. Psaras, W. K. Chai, and G. Pavlou, "Probabilistic in-network caching for information-centric networks," in Proceedings of the second edition of the ICN workshop on Information-centric networking, 2012.
[8] Y. Sun, S. K. Fayaz, Y. Guo, V. Sekar, Y. Jin, M. A. Kaafar, and S. Uhlig, "Trace-driven analysis of icn caching algorithms on video-on-demand workloads," in Proceedings of the 10th ACM International Conference on Emerging Networking Experiments and Technologies, 2014.
[9] N. Fotiou, G. F. Marias, and G. C. Polyzos, "Access control enforcement delegation for informationcentric networking architectures," in Proceedings of the second edition of the ICN workshop on Informationcentric networking, 2012.
[10] S. Singh, "A trust based approach for secure access control in information centric network," International Journal of Information and Network Security (IJINS), 2012.
[11] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertextpolicy attribute-based encryption," in Proceedings of the IEEE Symposium on Security and Privacy, 2007.
[12] S. Yu, K. Ren, and W. Lou, "Attribute-based ondemand multicast group setup with membership anonymity," in Proceedings of the 4th international conference on Security and privacy in communication netowrks, 2008.
[13] A. Lewko and B. Waters, "Decentralizing attributebased encryption," in EUROCRYPT, 2011.
[14] S. Arianfar, T. Koponen, B. Raghavan, and S. Shenker, "On preserving privacy in contentoriented networks," in Proceedings of the ACM SIGCOMM workshop on Information-centric networking, 2011.
[15] T. Nishide, K. Yoneyama, and K. Ohta, "Attributebased encryption with partially hidden encryptorspecified access structures," in Proceedings of the 6th international conference on Applied cryptography and network security, 2008.

INNO SPACE
SJIF Scientific Journal Impact Factor
Impact Factor: 7.542

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details